



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/483,127	01/14/2000	Alan Dowd	105.176US1	7964
21186 7590 01/30/2007 SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A. P.O. BOX 2938 MINNEAPOLIS, MN 55402			EXAMINER CRAIG, DWIN M	
			ART UNIT 2123	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE			MAIL DATE	
3 MONTHS			01/30/2007	
			DELIVERY MODE PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

09/483,127

Applicant(s)

DOWD ET AL.

Examiner

Dwin M. Craig

Art Unit

2123

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 October 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-42 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-25, 27-31, 33-36 and 38-42 is/are rejected.
- 7) ☒ Claim(s) 1-42 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 14 January 2000 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1-42 have been presented for appeal.

Response to Arguments

2. Appellant's arguments filed 10/27/06 have been fully considered but they are not persuasive.

2.1 Regarding Appellants' response to the application of Official Notice on page 11 of the 10/27/06 response, the Examiner will now provide documentary evidence regarding the limitations of playing a game over a network. "Prima's Official Strategy Guide, Star craft™ Expansion Set Brood War™" by Bart Farkas, hereafter referred to Farkas, teaches on pages 215-222 that Star Craft™ can be played using Battle.net™ over the internet, *which is a network* (see page 215) and there is an attacker (see page 222) and a defender (page 221).

2.2 Regarding Appellants' arguments regarding the combination of claims 1-8 under 35 U.S.C. § 103(a) on pages 13 & 14 of the 10/27/06 response, Appellants' argued that "*There is no simulator which simulates and analyzes networks based on network configuration data as described by Appellant and claimed in claims 1-8.*" The Examiner respectfully traverses this argument. *Lewis* teaches a network simulator, which has a mechanism to collect network configuration data, and *Shostack* teaches a database that contains network vulnerability information. The combination of *Lewis* and *Shostack* substantially teaches if not the exact *metes and bounds* of the presently presented claim language at least the functional equivalent of the claimed limitations.

Appellants' further argued on page 15 of the 10/27/06 response that, "*Although Shostack does describe a [sic] security vulnerabilities database (Table 1), the security vulnerabilities*

Art Unit: 2123

database is not part of the simulator, connected to a network configuration module, which is used to simulate and analyze networks based on the network configuration data..." the Examiner respectfully traverses Appellants' argument. The combination of *Lewis* and *Shostack* teach a simulator with a vulnerabilities database.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Appellants' further argue on page 15 of the 10/27/06 response that, "...*there is not teaching or suggestion in Shostack that each network vulnerability should include a service...*" *Shostack* teaches responding to attacks on electronic mail, (e-mail), see Col. 1 lines 59-63 more specifically "...For example, hackers are aware of vulnerabilities in software programs like electronic mail (e-mail)..." E-Mail provides a service on port 25 for SMTP (Simple Mail Transport Protocol) therefore *Shostack* meets the claimed limitation of a database having a network vulnerability that includes a service. Further, Col. 4 lines 33-46 teaches, "...*The database of security vulnerabilities includes a list of techniques used by hackers to gain unauthorized access to the network 20 and includes a catalog of known security weaknesses ins software programs stored on the network...*" these software programs include e-mail programs which provide services. Finally, *Shostack* teaches, Col. 5 lines 6-20 "...*a daemon which is a program intended to provide useful services...*"

Appellants' further argue on page 15 of the 10/27/06 response that, "*Finally as noted above, there must be some suggestion or motivation, wither in the reference themselves or in the*

Art Unit: 2123

knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. The Examiner stated that it would be obvious, to one of ordinary skill in the art at the time of the invention, to have used the network vulnerabilities database of Shostack with the network simulation database of Lewis because of the advantages provided by the database of Shostack to prevent damage to a computer network and systems...Appellant respectfully submits that the above passage is simply a statement of a problem that is purportedly solved by Shostack. It is not a suggestion or motivation to combine a reference that can determine network topology (Lewis) with a security modeling system that uses network configuration data and a security vulnerabilities database to simulate and analyze networks within a network simulator as described by Appellant and claimed in claims 1-8."

The Examiner respectfully traverses Appellants' argument. The combination would be obvious to an artisan or ordinary skill, the teaching of *Shostack* clearly teaches the advantage of providing the security database, which is to provide a quick, easy to access, and therefore useful method of reacting to an attack on a network system, at the time of the invention an artisan of ordinary skill, *in the hacking art* would have attack scripts that would perform multiple attacks on a network at once, the advantage of having a database of network vulnerabilities is to put the defending network in parity with the multiple attack methods of hackers at the time. Further, *Lewis* clearly teaches a modification with a data base, see Figure 1 #36 "Simulation Tool Database" and the descriptive text (see Col. 1 lines 39-52). The Examiner notes that the currently provided motivation does not include what has just been argued and therefore an updated form of the original rejection will be provided.

In regards to the rejections of claims 18-20 and Appellants' arguments thus presented, the Examiner respectfully traverses Appellants' arguments for the reasons presented.

2.3 Regarding Appellants' arguments regarding the combination of claims 10-25, 27-31, 33-36 and 40-42 under 35 U.S.C. § 103(a) on pages 16-21 of the 10/27/06 response Appellants presented three specific arguments,

1. That *Huff* fails to disclose a network vulnerabilities database, (page 17).
2. That *Huff* fails to disclose a mission objectives module (page(s) 18 & 19).

The Examiner respectfully traverses Appellants' arguments. Regarding the arguments that *Huff* fails to teach the functional equivalent of a Network Vulnerabilities Database, the Examiner points to the following teachings to *Huff*, which clearly disclose the functional equivalent of a *network vulnerabilities database* see Col. 7 lines 52-65 more specifically, "...*The DB historical support module 300 provides a **database** of historical information regarding previous threats and misuses...*" which is the functional equivalent of a *network vulnerabilities database*.

Regarding the argument that *Huff* fails to disclose a mission objectives module. The Examiner respectfully traverses Appellants' argument. *Huff* teaches, Col. 10 lines 24-32, more specifically, "...*the service request module can deploy data collection agents such as intrusion detection mission and collect data from collection agents...*" it would have been obvious to an artisan of ordinary skill, at the time of the invention to realize that the *objective* of the intrusion detection mission as clearly disclosed by *Huff* would be to detect an intrusion and therefore *Huff* teaches the functional equivalent of, if not substantially, a mission objective module.

Art Unit: 2123

2.4 Regarding the Appellants' response to Claims 9, 38 and 39, on pages 23-25 of the 10/27/06 responses, the previous rejection will be withdrawn and new grounds of rejection are being presented.

Claim Objections

3. Claims 1- 42 are objected to; taking claim 1 as an example, the preamble is pointing to a security modeling system however the elements set forth do not perform any modeling.

Clarification is requested.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 9, 38 and 39 are rejected under 35 U.S.C. 112, first paragraph, as based on a disclosure, which is not enabling. The rules system of the game, which is critical or essential to the practice of the invention, but not included in the claim(s) is not enabled by the disclosure.

See *In re Mayhew*, 527 F.2d 1229, 188 USPQ 356 (CCPA 1976).

4.1 Claims 9, 38 and 39 are rejected because the current claim language fails to disclose essential enabling components for a game such that an artisan of ordinary skill, without undue experimentation could make and/or use the invention. More specifically the current claim language and the specification fail to disclose the necessary structural cooperative components for use in a game such as what is the criteria for winning the game, what are the steps or phases

for a game turn, is the game taking place in real-time or is it turn based, etc... as necessary to practice the invention, it is unclear how an artisan of ordinary skill could make or use the claimed game, see MPEP section 2172.01, August 2006 edition.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

5. Claims 1-8, 18-20 and 40 are rejected under 35 USC § 103(a) as being unpatentable over US Patent 6,014,697 *Lewis* in view of US Patent 6,298,445 *Shostack*.

5.1 As regards independent claims 1 and 18 and using independent claim 1 as an example, *Lewis* discloses a network configuration module having network configuration data (Figure 1 reference 18, Col. 2 lines 4-6, 21-36, Figure 2 reference 42), and a simulator (Figure 1 reference 36, Col. 3 lines 17-24 and Col. 2 lines 51-56), coupled to the network configuration module

(Figure 1 references 34 and 36), *to simulate and analyze networks based on the network configuration data* (Col. 1 lines 39-52).

However *Lewis* does not expressly disclose the database having *network vulnerabilities*, *defense conditions that might close the vulnerability*, and *resource and state conditions needed to exercise the vulnerability*.

Shostack discloses a database that contains, *network vulnerabilities* (Figure 5 reference 92), *defense conditions that might close the vulnerability* (Col. 2 lines 48-54, “a database of known security vulnerabilities”), and *resource and state conditions needed to exercise the vulnerability* (Col. 6 lines 53-65, the Examiner notes that, “electronically disengage(ing) the intruder” will exercise a vulnerability).

Lewis and *Shostack* are analogous art because they are from the same field of endeavor of network management.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to have used the network vulnerability database methods of *Shostack* to modify the network configuration data collection and simulation database methods of *Lewis*.

The motivation for doing is from the teaching of *Shostack* which clearly teaches the advantage of providing the security database, which is to provide a quick, easy to access, and therefore useful method of reacting to an attack on a network system, at the time of the invention an artisan of ordinary skill, *in the hacking* art would have attack scripts that would perform multiple attacks on a network at once, the advantage of having a database of network vulnerabilities is to put the defending network in parity with the multiple attack methods of hackers at the time. Further, *Lewis* clearly teaches a modification with a database, see Figure 1

#36 "Simulation Tool Database" and the descriptive text (see Col. 1 lines 39-52), therefore, *Lewis* and *Shostack* are clearly compatible as teachings for combination and/or modification.

Therefore, it would have been obvious to combine *Shostack* with *Lewis* to obtain the invention as specified in claims 1-8, 18-20 and 40.

5.2 As regards dependent claim 2, *Lewis* does not expressly disclose network vulnerability, attack and exploitation data however, *Shostack* discloses network vulnerability, attack and exploitation data (Col. 2 lines 48-67 and Col. 3 lines 1-37).

5.3 As regards dependent claim 3, *Lewis* discloses a *database*, which contains tables, and the *database* of *Lewis* is being executed on a computer (Figure 1).

5.4 As regards dependent claim 4, *Lewis* discloses *output of data from a network discovery tool* (Figure 1 references 14, 18, 20 and 22).

5.5 As regards dependent claim 5, *Lewis* discloses a *user interface* (Figure 1 references 22 and 40).

5.6 As regards dependent claim 6, *Lewis* does not expressly disclose *a means for receiving the network vulnerability, attack and exploitation data*.

Shostack discloses *a means for receiving the network vulnerability, attack and exploitation data* (Figure 7).

5.7 As regards dependent claim 7, *Lewis* does not expressly disclose an *attacker and a defender interface*.

Shostack discloses the functional equivalent of an *attacker and defender interface* (Figure 1 reference(s) 8 and 16).

5.8 As regards dependent claim 8 *Lewis* discloses a “*portable*” security modeling system, more specifically in Col. 4 lines 29-39 disclose the use of the *Sniffer by Network General Corporation*, it is known through the personal knowledge of the Examiner that the *Sniffer* product is provided on stand alone *portable* computer systems as well as CDROM encoded computer readable media that can be utilized on *portable* computer systems.

5.9 As regards dependent claim 19 *Lewis* discloses a *network discovery tool* (Figure 1 reference 14).

5.10 As regards dependent claim 20 *Lewis* discloses *receiving a file* (Figure 1 references 24, 26, 28, 30, 32 and 34 and Col. 3 lines 25-33).

5.11 Regarding claim 40, see the rejection of claim 1 above.

6. Claims 10-25, 27-31, 33-36 and 40-42 are rejected under 35 USC § 103(a) as being unpatentable over US Patent 6,014,697 to *Lewis* in view of US Patent 6,408,391 to *Huff*.

6.1 As regards independent claims 10, 18, 28, 34 and 40 and using independent claim 10 as an example, *Lewis* discloses a *network configuration module having network configuration data* (Figure 1 reference 18, Col. 2 lines 4-6, 21-36, Figure 2 reference 42), and a *simulator* (Figure 1 reference 36, Col. 3 lines 17-24 and Col. 2 lines 51-56), *coupled to the network configuration module* (Figure 1 references 34 and 36), *to simulate and analyze networks based on the network configuration data* (Col. 1 lines 39-52).

However, *Lewis* does not expressly disclose a *mission objective module, with critical resource information used to determine network components that are involved in specific attack scenarios and a network vulnerabilities database*.

Huff discloses a mission objective module, with critical resource information and specific attack scenarios (Abstract, Figure 3 references 320, 322 and 324, Col. 3 lines 49-58, Col. 8 lines 34-56, Col. 9 lines 6-17, Col. 10 lines 3-67, Col. 11 lines 1-6, Col. 11 lines 22-67 and Col. 12 lines 1-24) and *Huff* substantially teaches critical resource information used to determine network components that are involved in a specific attack scenario (Figure 1 items 106 and 114, 112, 104 & 108 are all network components see also Figure 4 and see also Col. 3 lines 38-58 regarding the different *nodes* of the network, these nodes are critical resources and the agents on them are there for protection, see also Col. 4 lines 8-33 more specifically “The computer architecture includes determining means for determining that an unauthorized operation has occurred at an audited computer...” the audited computer is the functional equivalent of *to determine network components that are involved in specific attack scenarios*) and *Huff* teaches, Col. 10 lines 24-32, more specifically, “...the service request module can deploy data collection agents such as intrusion detection mission and collect data from collection agents...” it would have been obvious to an artisan of ordinary skill, at the time of the invention to realize that the *objective* of the intrusion detection mission as clearly disclosed by *Huff* would be to detect an intrusion and therefore *Huff* teaches the functional equivalent of, if not substantially, a mission objective module. *Huff*, clearly teaches the functional equivalent of a network vulnerabilities database see Col. 7 lines 52-65 more specifically, “...The DB historical support module 300 provides a **database** of historical information regarding previous threats and misuses...” which is the functional equivalent of a network vulnerabilities database.

Lewis and *Huff* are analogous art because they are from the same field of endeavor of network management.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to have used the network management and database methods of *Lewis* in combination with the network vulnerabilities and protection methods of *Huff*.

The motivation for doing so is provided by *Huff* in that it would be advantageous because, *prior art systems can be circumvented before a human system administrator takes action* (*Huff*, Col. 11 lines 2-6) thus, having an automated network protection system provides for better network security and protection of critical data. Further there is a need that exists for a system that can automatically take defensive steps to stop misuse or intrusion after it is detected and even take offensive steps to stop a network intruder (*Huff*, Col. 2 lines 48-53).

Therefore, it would have been obvious to combine *Huff* with *Lewis* to obtain the invention as specified in claims 10-25, 27-31, 33-36 and 40-42.

6.2 As regards dependent claim 11 *Lewis* does not expressly disclose *network vulnerability, attack and exploitation data*.

Huff discloses *network vulnerability, attack and exploitation data* (Col. 7 lines 52-65).

6.3 As regards dependent claim 12 *Lewis* does not expressly disclose *network vulnerability, attack and exploitation data is stored in database tables processed by a computer*.

Huff discloses a database with network vulnerability data, attack data and exploitation data, stored and processed by a computer (Figure 3 reference 286).

6.4 As regards dependent claim 13 *Lewis* discloses a *GUI* (Col. 2 lines 51-56).

6.5 As regards dependent claim 14 *Lewis* discloses *goals, expectations and constraints for simulating a network* (Col. 1 lines 39-53).

Art Unit: 2123

6.6 As regards dependent claim 15 *Lewis* discloses *means for receiving network data* (Figure 1 reference 16).

6.7 As regards dependent claim 16 a *Lewis* discloses a “*portable*” security modeling system, more specifically in Col. 4 lines 29-39 disclose the use of the *Sniffer by Network General Corporation*, it is known through the personal knowledge of the Examiner that the *Sniffer* product is provided on stand alone *portable* computer systems as well as CDROM encoded computer readable media that can be utilized on *portable* computer systems.

6.8 As regards dependent claim 17 *Lewis* does not expressly disclose *attackers and defenders*.

Huff discloses *attackers and defenders* (Col. 2 lines 58-65, *et seq.*) *Huff* also discloses a GUI for the defender (Col. 7 lines 45-47).

6.9 As regards dependent claim 19 *Lewis* discloses a *network discovery tool* (Figure 1 reference 14).

6.10 As regards dependent claim 20 *Lewis* discloses *receiving a file* (Figure 1 references 24, 26, 28, 30, 32 and 34 and Col. 3 lines 25-33).

6.11 As regards dependent claim 21, *Lewis* does not expressly disclose *receiving mission objectives, storing and simulating a network based on those objectives*.

Huff discloses *receiving mission objectives, storing and simulating a network based on those objectives* (Col. 9 lines 6-17, Col. 9 lines 33-53, Col. 10 lines 33-44, “increase the auditing level being performed by the intrusion detection mission”, *et seq.*).

6.12 As regards dependent claim 22, *Lewis* does not expressly disclose modifying a GUI.

Huff discloses modifying a GUI based on activity on the network (Figure 4, Col. 7 lines 45-47).

6.13 As regards dependent claims 23-25 *Lewis* does not expressly disclose dynamic interaction with an attacker.

Huff discloses dynamically interacting with an attacker, in real time and interacting with the security modeling system (Col. 2 lines 64-66, Col. 3 lines 23-29, Col. 7 lines 52-65 *et seq.*).

6.14 As regards dependent claim 27 *Lewis* discloses updating a database (Figure 1 reference 34 and Figure 2 reference 48, Col. 3 lines 29-33).

6.15 As regards dependent claim 29 *Lewis* does not expressly disclose receiving information from a defender.

Huff discloses receiving information from a defender (Col. 11 lines 23-45).

6.16 As regards dependent claim 30 *Lewis* discloses *goals, expectations and constraints for simulating a network* (Col. 1 lines 39-53).

6.17 As regards dependent claim 31 *Lewis* does not expressly disclose modifying a GUI.

Huff discloses modifying a GUI based on activity on the network (Figure 4, Col. 7 lines 45-47).

6.18 As regards dependent claim 33 *Lewis* does not expressly disclose receiving commands.

Huff discloses *receiving commands to change the attacker/defender nodes, service functionality and exploit vulnerabilities* (Figure 3-5 and in figure 5 reference 272 and 272' "response engines" which send commands to the "agents" Col. 13 lines 30-43).

6.19 As regards dependent claims 35 and 36, *Lewis* does not expressly disclose *mission objective tables, mission files tables and mission service tables*.

Huff discloses a database (Figure 3 reference 286, Figure 5 references 300 and 300' and Col. 7 lines 18-65), the Examiner notes that all databases have tables or data stored in tabular format. *Huff* further discloses the functional equivalent of *mission objective tables*, *mission files tables* and *mission service tables* (Col. 9 lines 54-67, Col. 10 and Col. 11 lines 1-6, *et seq.*).

6.20 As regards dependent claims 41 and 42, *Lewis* does not expressly disclose *mission objectives*.

Huff discloses *mission objectives* (Col. 11 lines 22-45).

6.21 Regarding independent claim 18, which is substantially rejected using the rejection of claim 10 above.

Lewis does not expressly disclose, *wherein each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, etc...*

However, *Huff* teaches figure 4 under the banner "SK Security Monitor" see "io: FTP Password decoding – port 21" the port 21 FTP is a service, further *Huff* discloses, (Col. 12 lines 57-67 and Col. 13 lines 1-15) and more specifically the discussion of the "*Trojan Horse*" Trojan horses will open up *services* like Telnet and FTP in order to communicate with the originator.

6.22 Regarding independent claim 28, which is substantially rejected using the rejection of claim 10 see above.

Lewis does not expressly disclose, *responding to the network attacker, wherein responding to the attacker includes imposing barriers, providing response messages and protecting the network*.

However, *Huff* teaches, *responding to the network attacker*, (Col. 12 lines 47-67 and Col. 13 lines 1-15) *wherein responding to the attacker includes imposing barriers, providing response messages and protecting the network* (Col. 11 lines 22-60).

6.23 Regarding independent claim 34, which is substantially rejected using the rejection of claim 10 above.

Lewis does not expressly disclose, *a graphical user interface which operates with the simulator to allow input and output to clients*.

Huff teaches, (Figure 4 and the descriptive text).

7. Claims 9, 38 and 39 are rejected under 35 USC § 103(a) as being unpatentable over US Patent 6,014,697 *Lewis* in view of US Patent 6,408,391 *Huff* and in further view of “Prima’s Official Strategy Guide, Star craft Expansion Set Brood War™” by Bart Farkas, hereafter referred to Farkas.

7.1 As regards independent claim 9, *Lewis* discloses *a network configuration module having network configuration data* (Figure 1 reference 18, Col. 2 lines 4-6, 21-36, Figure 2 reference 42), and *a simulator* (Figure 1 reference 36, Col. 3 lines 17-24 and Col. 2 lines 51-56), *coupled to the network configuration module* (Figure 1 references 34 and 36), *to simulate and analyze networks based on the network configuration data* (Col. 1 lines 39-52).

However *Lewis* does not expressly disclose the *database having network vulnerabilities*.

Huff discloses *a database having network vulnerabilities* (Col. 7 lines 52-65). *Huff* also discloses an interactive GUI (Figure 4, Col. 7 lines 45-60) and *Huff*, clearly teaches the functional equivalent of *a network vulnerabilities database* see Col. 7 lines 52-65 more

specifically, "...*The DB historical support module 300 provides a database of historical information regarding previous threats and misuses...*" which is the functional equivalent of a *network vulnerabilities database*.

Lewis and *Huff* are analogous art because they are from the same field of endeavor of network management.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to have used the network management and database methods of *Lewis* in combination with the network vulnerabilities and protection methods of *Huff*.

The motivation for doing so is provided by *Huff* in that it would be advantageous because, *prior art systems can be circumvented before a human system administrator takes action* (*Huff*, Col. 11 lines 2-6) thus, having an automated network protection system provides for better network security and protection of critical data.

Therefore, it would have been obvious to combine *Huff* with *Lewis* to obtain the invention as specified in claims 9, 38 and 39.

As regards the limitation of independent claim 9 that the simulator is used as a game. At the time the invention was made *Real Time Simulation (RTS) Games* were widely available, more specifically games like *StarCraft™* and *Warcraft II™* by *Blizzard® Entertainment Inc.* were available and disclosed interactive simulation(s) where an attacker and a defender could attack each other using a GUI over a network. More specifically, *Blizzard™ Entertainment Inc.* actually provided specific network servers to facilitate these networked games known as *Battle.net™* servers, therefore, it would have been obvious, to one of ordinary skill in the art, at the time the invention was made to have taken the claimed invention and use the *network*

simulator as a *RTS* game see “Prima’s Official Strategy Guide, Star craft™ Expansion Set Brood War™”, Farkas, teaches on pages 215-222 that Star Craft™ can be played using Battle.net™ over the internet, *which is a network* (see page 215) and there is an attacker (see page 222) and a defender (page 221) and that the game Star Craft™ includes a Graphical User Interface (see figures, 7-02, 7-03 and 7-04 on pages 220, 221 and 222 respectively).

7.2 As regards dependent claim 38, *Lewis* does not expressly disclose an *attacker* interface.

However, *Huff* discloses an *attacker interface* (Figure 1 reference 130) and a *Defender interface* (Figure 4, Col. 7 lines 45-60).

7.3 As regards dependent claim 39 *Lewis* does not expressly disclose *mission objectives*.

Huff discloses *receiving mission objectives, storing and simulating a network based on those objectives* (Col. 9 lines 6-17, Col. 9 lines 33-53, Col. 10 lines 33-44, “increase the auditing level being performed by the intrusion detection mission”, *et seq.*).

Possible Allowable Subject Matter

8. Regarding claims 26, 32 and 37, the Examiner set for the reasons for indication of allowable subject matter in the previous office action.

Conclusion

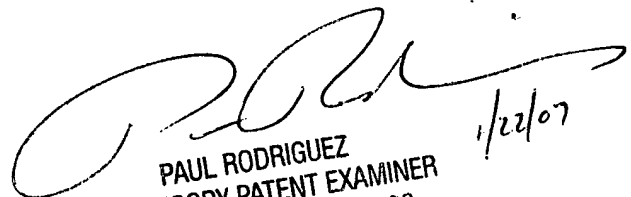
9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dwain M. Craig whose telephone number is (571) 272-3710. The examiner can normally be reached on 10:00 - 6:00 M-F.

Art Unit: 2123

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Paul L. Rodriguez can be reached on (571) 272-3753. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Dwin McTaggart Craig


PAUL RODRIGUEZ
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100
1/22/07